AMENDMENTS TO THE CLAIMS

Please cancel claims 29, 31-34, 37, 47 and 50-52 without prejudice or disclaimer of their underlying subject matter.

1-20. (canceled)

Please amend the claims as follows.

21. (currently amended) A random number generation apparatus comprising:

a pick-up block structurally adapted to capture living body information and to output a pick-up signal depicting said living body information;

A/D converter structurally adapted to convert said pick-up signal into a gray scale image composed of a plurality of gray scale pixels, a gray scale pixel of said plurality gray scale of pixels having a gray scale pixel value expressed by a plurality of bits;

a image processor structurally adapted to generate a binary image from said gray scale image, a binary image pixel of said binary image being generated by comparing said gray scale pixel value with an average of gray scale pixel values for said plurality of gray scale pixels, said binary image pixel having a binary pixel value expressed by a single bit; and

an encryption block having a random number generator structurally adapted to generate a random number sequence from said pick-up signal when no living body information is captured by said pick-up block, said random number sequence being generated using either said gray scale pixel value or said binary pixel value,

said gray scale pixel being located at a start address,

said random number generator generating said random number sequence by extracting the least significant bit of said gray scale pixel value and the least significant bit for each of the gray scale pixel values of a predetermined number of gray scale pixels succeeding said gray scale pixel,

said start address being located at an appropriate position in said gray scale image,

said appropriate position being at a horizontal address and a vertical address,

said horizontal address being a value expressed by said gray scale pixel value, and

said vertical address being a value expressed by another gray scale pixel value of another gray scale pixel of said plurality gray scale pixels that is adjacent said gray scale pixel.

22. (previously presented) A random number generating apparatus as claimed in Claim 21, wherein said living body information is a fingerprint.

23. (previously presented) A random number generating apparatus as claimed in Claim 21, wherein said binary image is composed of a plurality of binary image pixels.

24. (previously presented) A random number generating apparatus as claimed in Claim 21, further comprising memory structurally adapted to store said gray scale image.

25. (previously presented) A random number generating apparatus as claimed in Claim 21, further comprising memory structurally adapted to store said binary image.

26. (previously presented) A random number generating apparatus as claimed in Claim 21, wherein said plurality of gray scale pixels is the number of gray scale pixels for the entire gray scale image.

27. (currently amended) A random number generating apparatus as claimed in Claim 21, wherein said plurality of gray scale pixels is the number of gray scale pixels located at a segment of said gray scale image in a predetermined range from said gray scale pixel.

28. (currently amended) A random number generating apparatus as claimed in Claim 21, wherein black portions of said binary image represent convex portions of said living body information and the white portions of said binary image represent concave portions of said living body information.

29. (canceled)

30. (currently amended) A random number generating apparatus as claimed in Claim 21~~Claim 29~~, wherein said appropriate position ~~start address~~ is located at a predetermined position in said gray scale image.

31-34. (canceled)

35. (previously presented) A random number generating apparatus as claimed in Claim 21, wherein said encryption block further comprises:

encryption means structurally adapted to perform encryption using an encryption key.

36. (previously presented) A random number generating apparatus as claimed in Claim 35, wherein said encryption key is said random number sequence.

37. (canceled)

38. (currently amended) A random number generating apparatus as claimed in Claim 35 ~~Claim 37~~, wherein said encryption means employs the RSA encryption method for generating said encryption key according to two prime numbers and generates said two prime numbers according to said random number generated by said random number generating means, so that said two prime numbers are used for generating said encryption key.

39. (previously presented) A random number generating apparatus as claimed in Claim 35, further comprising:

a fingerprint identification block structurally adapted to identify an individual by comparing said binary image with registered image information.

40. (previously presented) A random number generating apparatus as claimed in Claim 39, wherein said fingerprint identification block performs an encryption of a plain text using said encryption key when said individual is identified.

41. (currently amended) A random number generating method comprising steps of:

capturing living body information;

outputting a pick-up signal depicting said living body information;

converting said pick-up signal into a gray scale image composed of a plurality of gray scale pixels, a gray scale pixel of said plurality gray scale of pixels having a gray scale pixel value expressed by a plurality of bits;

generating a binary image from said gray scale image, a binary image pixel of said binary image being generated by comparing said gray scale pixel value with an average of gray scale pixel values for said plurality of gray scale pixels, said binary image pixel having a binary pixel value expressed by a single bit; and

generating a random number sequence from said pick-up signal when no living body information is captured by said pick-up block, said random number sequence being generated using either said gray scale pixel value or said binary pixel value,

said gray scale pixel being located at a start address,

said random number sequence being generated by extracting the least significant bit of said gray scale pixel value and the least significant bit for each of the gray scale pixel values of a predetermined number of gray scale pixels succeeding said gray scale pixel,

said start address being located at an appropriate position in said gray scale image,

said appropriate position being at a horizontal address and a vertical address,

said horizontal address being a value expressed by said gray scale pixel value and,

said vertical address being a value expressed by another gray scale pixel value of another gray scale pixel of said plurality gray scale pixels that is adjacent said gray scale pixel.

42. (previously presented) A random number generating method as claimed in Claim 41, wherein said living body information is a fingerprint.

43. (previously presented) A random number generating method as claimed in Claim 41, wherein said binary image is composed of a plurality of binary image pixels.

44. (previously presented) A random number generating method as claimed in Claim 41, wherein said plurality of gray scale pixels is the number of gray scale pixels for the entire gray scale image.

45. (currently amended) A random number generating method as claimed in Claim 41, wherein said plurality of gray scale pixels is the number of gray scale pixels located at a segment of said gray scale image in a predetermined range from said gray scale pixel.

46. (currently amended) A random number generating method as claimed in Claim 41, further comprising the step of: ~~a fingerprint identifier structurally adapted to~~

identifying said binary image.

47. (canceled)

48. (currently amended) A random number generating method as claimed in Claim 41 ~~Claim 47~~, wherein said appropriate position ~~start address~~ is located at a predetermined position in said gray scale image.

49-52. (canceled)

53. (currently amended) A random number generating method as claimed in Claim 41, further comprising the step of:

performing encryption using an encryption key.

54. (previously presented) A random number generating method as claimed in Claim 53, wherein said encryption key is said random number sequence.

55. (previously presented) A random number generating method as claimed in Claim 53, wherein said encryption key is according to said random number sequence.

56. (currently amended) A random number generating method as claimed in Claim 55, wherein said step of performing encryption further comprises:

employing the RSA encryption method to generate said encryption key according to two prime numbers and generates said two prime numbers according to said random number generated by said random number generating means, so that said two prime numbers are used for generating said encryption key.

57. (previously presented) A random number generating method as claimed in Claim 53, further comprising the step of:

identifying an individual by comparing said binary image with registered image information.

58. (previously presented) A random number generating method as claimed in Claim 57, further comprising:

performing an encryption of a plain text using said encryption key when said individual is identified.